(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 334 616 B1**

(12) # EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification : **26.10.94 Bulletin 94/43**

(51) Int. Cl.[5] : **G07F 7/10,** G07C 9/00

(21) Application number : **89302812.6**

(22) Date of filing : **21.03.89**

(54) **Method and system for personal identification.**

(30) Priority : **21.03.88 US 170734**

(43) Date of publication of application : **27.09.89 Bulletin 89/39**

(45) Publication of the grant of the patent : **26.10.94 Bulletin 94/43**

(84) Designated Contracting States : **DE FR GB IT NL**

(56) References cited :
EP-A- 0 216 298
EP-A- 0 225 010
US-A- 4 636 622

(73) Proprietor : **Leighton, Frank T.**
965 Dedham Street
Newton Center, MA 02159 (US)
Proprietor : **Micali, Silvio**
224 Upland Road
Cambridge, MA 02140 (US)

(72) Inventor : **Leighton, Frank T.**
965 Dedham Street
Newton Center, MA 02159 (US)
Inventor : **Micali, Silvio**
224 Upland Road
Cambridge, MA 02140 (US)

(74) Representative : **Lawrence, Malcolm Graham et al**
Hepworth, Lawrence & Bryer
2nd Floor, Gate House South
Westgate Road
Harlow Essex CM20 1JN (GB)

EP 0 334 616 B1

Description

TECHNICAL FIELD

The present invention relates generally to personal identification schemes and more particularly to a method and system for issuing authorized personal identification cards and for preventing unauthorized use thereof during transaction processing.

BACKGROUND OF THE INVENTION

Password-based protection schemes for credit cards or other personal identification cards are well-known in the prior art. Such cards typically Include a memory comprising a magnetic tape or other storage media affixed to the card. They may also Include a data processing capability in the form of a microprocessor and an associated control program. In operation, a card issuer initially stores in the memory a personal identification number, ie, a secret password, as well as a value representing a maximum dollar amount. To effect a transaction, the card is placed in a terminal and the user is required to input his or her password. If the terminal verifies a match between the user-inputted password and the password stored on the card, the transaction is allowed to proceed. The value of the transaction is then subtracted from the value remaining on the card, and the resulting value represents the available user credit.

Techniques have also been described in the prior art for protecting against the illegitimate issuance of credit cards such as the type described above. In US Patent No 4,453,074 to Weinstein, each such card has stored therein a code which is the encryption of a concatenation of a user's secret password and a common reference text. The encryption is derived in an initialization terminal through the use of a private key associated with the public key of a public-key cryptosystem key pair. In operation, a cardholder presents his or her card to a transaction terminal. The terminal decrypts the stored code on the card in accordance with the public key of the public-key cryptosystem pair. A transaction is effected only if the stored code decrypts into the user password, inputted on a keyboard by the cardholder, and the common reference text.

While the method described in the Weinstein patent provides an adequate protection scheme for preventing the fraudulent issuance of credit cards, this scheme requires each user to have a secret or "private" password which must be memorized and Inputted into the transaction terminal. Weinstein also requires additional circuitry for concatenating the user's secret password with the common reference text. This latter requirement, while purportedly required to insure the integrity of the protection scheme, increases the complexity and the cost of the system.

It would therefore be desirable to provide an improved method for issuing personal identification cards using a public-key cryptosystem in which a "secret" password need not be memorized by the authorized user or concatenated with a common reference text to maintain the system security.

According to one aspect of the present invention, there is provided a system for issuing authorized personal identification cards and for preventing unauthorized use thereof, comprising:

issuing terminal means for issuing a plurality of personal identification cards; each of said cards having stored therein a first data string with a portion thereof derived from a physical characteristic of an authorized user of the card, each of said cards also having stored therein a signature derived from a second data string using a private key of a public-key cryptosystem pair, the public-key cryptosystem pair also having a public key, the second data string being derived from the first data string using a predetermined one-way function and having a length substantially less than the length of the first data string; and

transaction terminal means including at least one transaction terminal for receiving a personal identification card offered to effect a transaction using the transaction terminal, the personal identification card having the first data string and a received signature stored therein, wherein the transaction terminal comprises means, using the public key of the public-key cryptosystem pair, for verifying that the received signature can be generated from the first data string, means responsive to the verifying means for generating a representation from the first data string, and means for displaying the representation and an indication of whether the received signature can be generated from the first data string to enable an operator of the transaction terminal to verify that the user of the offered personal identification card is authorized to effect a transaction.

It will be appreciated that it is very difficult to create a valid signature for any personal data without the proper private key, although it is simple for anyone to verify whether or not the signature for a password (first data string) on the card is authentic, even without the private key. Only a card issuer can thus make a valid card and only a user with matching personal characteristics can use the card.

In the preferred embodiment, the password includes data representing a pictorial representation of a physical characteristic (eg, the face, fingerprint, voice sample or the like) of the authorized user. Alternatively, or in addition to the pictorial representation data, the password may contain other data pertinent to the user, such as the user's age, address, nationality, security clearance, bank account balance, employer, proof of ownership, or the like. The password may also include one or more codewords, each of the codewords authorizing a specific transaction such as

permission to receive certain funds on a certain date, permission to see classified documents, permission to enter into a country on a certain date (ie, a visa), attestation to perform certain acts, or the like. Although not meant to be limiting, the personal identification card may be a credit card, a driver's licence, a passport, a membership card, an age verification card, a bank card, a security clearance card, a corporate identification card or a national identification card.

The generation of the digital signature preferably includes the steps of multiplying the mapped password (the second data string) "Q" by each of the four factors ±1 modulo "M" and ±2 modulo "M", where $M=P_1 \cdot P_2$. As used herein, "M" refers to the public key of the public-key cryptosystem pair and (P_1,P_2) refers to the private key thereof, where "P_1" and "P_2" are secret prime numbers which are preselected such that only one of the four values ±Q mod M and ±2Q mod M is a quadratic residue modulo "M". According to the digital signing routine, the four values ±Q mod M and ±2Q mod M are evaluated to determine which of these values is a quadratic residue modulo "M". The square root of the quadratic residue is then computed to generate the signature. Because the square root computation is extremely difficult to carry out without knowing the factorization of the secret prime numbers of the private key, unauthorized third parties are not capable of producing a card "signature" which, when digitally verified at the transaction terminal, can be shown to have been generated from the mapped password on the received personal identification card.

In accordance with another aspect of the present invention, there is provided a system for allowing authorized users of personal identification cards to effect transactions via at least one transaction terminal, comprising a plurality of cards each having stored therein a signature which is the digital signature of a second data string, the second data string being derived from a first data string derived from a physical characteristic associated with a respective user, the second data string being derived from the first data string using a predetermined one-way function and having a length substantially less than the length of the first data string, the signature stored in each of said cards having been derived with the same private key of a public-key cryptosystem pair also having a public key; and at least one transaction terminal having means for controlling:

(1) the retrieval of the first data string and the signature stored in an inserted card;

(2) the digital verification of the signature with the use of the public key of the public-key cryptosystem pair;

(3) the generation of a pictorial representation from the first data string; and

(4) the effecting of a transaction only if the signature is verified and the pictorial representation matches the user.

According to a further aspect of the present invention, there is provided a terminal for initializing personal identification cards to be used with at least one transaction terminal, each card having a memory therein, comprising means for assigning a first data string having a portion thereof which is derived from a physical characteristic of a user whose card is to be initialized, means for mapping the first data string with a predetermined one-way function to generate a second data string having a length substantially less than the length of the first data string, means for deriving a digital signature from the second data string, the signature of each user being derived with use of a private key of a public-key cryptosystem pair also having a public key, and means for controlling the storing in a user card of the respective derived digital signature.

According to a still further aspect of the present invention, there is provided a personal identification card for use in effecting transactions via at least one transaction terminal, comprising a body portion, a memory within said body portion for storing a signature, said signature being the digital signature of a second data string derived from a first data string having at least a portion thereof being derived from a physical characteristic of a respective card user, the second data string being derived from the first data string using a predetermined one-way function and having a length substantially less than the length of the first data string, wherein said signature is derived from the second data string with the private key of a public-key cryptosystem pair.

According to a yet further aspect of the present invention, there is provided a method for enabling an authorized user of a personal identification card to effect a transaction using a transaction terminal, the personal identification card having user-characteristic data derived from a physical characteristic of the authorized user and which need not be retained secret, and a signature of the user-characteristic data derived from a private key of a public-key cryptosystem pair, the public-key cryptosystem pair also including a public key, comprising the steps of:

receiving the personal identification card at the transaction terminal;

digitally verifying, using the public key, whether the signature on the personal identification card received at the transaction terminal can be generated from the user-characteristic data; and

if the signature can be generated from the user-characteristic data using the public key, displaying a representation of the user-characteristic data on a display of the transaction terminal to enable an operator thereof to verify that the user is authorised to effect a transaction using the personal card.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following Description taken in conjunction with the accompanying Drawings in which:

FIGURE 1 is a schematic representation of one type of personal identification card according to the invention, the card having a picture of a physical characteristic of an authorized user of the identification card;

FIGURE 1A is a diagrammatic representation of a portion of a magnetic stripe of the personal identification card of FIGURE 1 showing a "password" generated in part from the picture on the identification card;

FIGURE 2 is a general flowchart diagram of the preferred method of the present invention for issuing an authorized personal identification card such as shown in FIGURE 1;

FIGURE 3 is a detailed flowchart diagram of the digital signing routine of FIGURE 2;

FIGURE 3A is a flowchart diagram of a routine for selecting the secret prime numbers of the private key (P_1,P_2);

FIGURE 4 is a general flowchart diagram of the preferred method of the present invention for preventing unauthorized use of the personal identification card of FIGURE 1 which is issued according to the method of FIGURE 2;

FIGURE 5 is a detailed flowchart diagram of the digital verifying routine of FIGURE 4; and

FIGURE 6 is a block diagram of a representative multi-Issuer system according to the present invention.

DETAILED DESCRIPTION

With reference now to the drawings wherein like reference numerals designate like or similar parts or steps, FIGURE 1 is a schematic representation of a personal identification card 10 for use according to the present invention for effecting transactions via a transaction terminal. As noted above, the term "personal identification card" according to the present invention is to be read expansively and is deemed to cover credit cards or other commonly known forms of identification such as a passport, a driver's license, a membership card, an age identification card, a security clearance card, a corporate identification card, a national Identification card, or the like.

Personal identification card 10 in FIGURE 1 is a driver's license. Card 10 includes a body portion 12 having a display 14 and a memory 16. Although not meant to be limiting, the memory 16 is preferably a magnetic stripe or similar media, or an electronic memory such as a PROM, affixed to or embedded in the card in a known manner. The personal identification card may or may not include an integral microprocessor embedded in the body portion. As seen in FIGURE 1, the display 14 of the personal identification card 10 supports a pictorial representation 18 of a physical characteristic of the authorized user; eg, the user's face. Of course, the display 14 may also display pictorial representations of other physical features of the user such as the user's fingerprint or palm print.

Referring now to FIGURE 1A, according to the present invention the memory 16 of the personal identification card 10 preferably includes a "password" 20 unique to the authorized user and having a portion 20a thereof which is generated from a representation of some non-secret or "public" characteristic of the user. As used herein, the term "non-secret" refers to the fact that the representation of the authorized user, such as the user's face, is readily ascertainable by viewing and comparing the personal identification card and the authorized user directly. In the preferred embodiment, the section 20a of the password is a digital bitstream representing a digitized version of the pictorial representation 18 on the personal identification card 10.

As also seen in FIGURE 1A, the password 20 may include a portion 20b having data representing one or more personal facts about the authorized user such as the user's age, address, nationality, security clearance, employer, bank account balance, eye colour, height, weight, mother's maiden name, or any other such information. This information may or may not be public. Moreover, the password 20 may further include a portion 20c having one or more codewords, each of the codewords authorizing a specific transaction such as permission to enter a country on a certain date, permission to receive certain funds on a certain date, permission to review certain classified documents, or one or more other such specific transactions. Of course, the password 20 may include one or more of the predetermined types of data, 20a, 20b, and/or 20c, shown in FIGURE 1A.

As also seen in FIGURE 1A, the memory 16 of the personal identification card 10 also includes a signature 22, which, as will be described in more detail below, is derived from the password 20 using the private key of a "public-key cryptosystem" key pair. A "public-key cryptosystem" is a well known security scheme which includes two "keys", one key which is public (or at least the key-pair owner does not really care if it becomes public) and one key which is private or non-public. All such public-key cryptosystem pairs include a common feature - the private key cannot be determined from the public key.

Referring now to FIGURE 2, a general flowchart diagram is shown of the preferred method of the present invention for issuing an authorized personal identification card 10 such as shown in FIGURE 1. At step 30, the card issuer collects the necessary personal

data from a card applicant. Although not meant to be limiting, this data preferably includes a pictorial representation of a physical characteristic of the authorized user. For example, the date may include a photograph of the card applicant. At step 32, the photograph, other personal data and/or code authorizations are processed to generate a password as described above in FIGURE 1A.

At step 34, the password is mapped with a predetermined one-way function "F" to generate a mapped password "Q" which may have a length substantially less than the length of the password. This "mapping" step is typically required to reduce the length of the digital bitstream comprising the password, especially when a digitized photograph of the authorized user is stored therein. By way of example only, the predetermined one-way function "F" may be any one or more of several well-known hashing functions such as one obtainable from the DES scheme or the Goldwasser, Micall & Rivest scheme. Alternatively, the function "F" may be an identity function which simply transfers the password through step 34 without modification. The identity function might be used where the password length is sufficiently smaller than the available storage capability of the memory 16.

At step 36, the method continues to "digitally sign" the mapped password "Q" with a private key (P_1,P_2) of a public-key cryptosystem pair to generate a so-called "signature". As will be described in more detail below, in the preferred embodiment "P_1" and "P_2" are secret prime numbers and the public-key cryptosystem pair includes a public key "M" which is equal to "$P_1 \cdot P_2$". At step 38, the method encodes the password (as opposed to the mapped password) and the signature with an error-corecting code to generate an encoded password/signature. Step 38 insures that the card 10 will be usable even if some of its data is destroyed. At step 40, the encoded password/signature is stored on the personal identification card in the manner substantially as shown in FIGURE 1A.

Although not shown in detail in FIGURE 2, it should be appreciated that the card issuer may digitally sign one or more digital signatures on the card 10 at one or more different times using different public-key cryptosystem pair keys. The card could then function as a passport with each signature derived from a different cryptosystem key pair corresponding to a different country (ie, a visa). It may also be desirable in the method of FIGURE 2 to Include an additional encryption step wherein the password is encrypted with a predetermined function prior to the mapping step and/or where the signature itself is encrypted. This enables the card to carry information which is desired to be maintained highly confidential even if the card were lost or stolen.

Referring now to FIGURE 3, a detailed flowchart diagram is shown of the preferred digital signing routine of the present invention. As described above, "M" is the public key of the public-key cryptosystem and (P_1,P_2) is the private key thereof. According to the routine, the secret prime numbers "P_1" and "P_2" are selected at step 42 such that when the mapped password Q is multiplied by four predetermined factors, ± 1 modulo "M" and ± 2 modulo "M", one and only one of the resulting values $\pm Q \bmod M$ and $\pm 2Q \bmod M$ is a quadratic residue modulo "M". The security of the preferred digital signing routine is based primarily on the fact that it is extremely difficult to compute the square root of the quadratic residue modulo "M" without knowing the factorizatlon of $M = P_1 \cdot P_2$.

Referring back to FIGURE 3, at step 44 the mapped password "Q" is multiplied by each of the factors $\pm 1 \bmod M$ and $\pm 2 \bmod M$. The routine continues at step 46, wherein each of the resulting values $\pm Q \bmod M$ and $\pm 2Q \bmod M$ are evaluated to locate the quadratic residue mod "M". When this value is located, the routine computes the square root thereof at step 48 to generate the digital signature.

Although not shown in detail, it should be appreciated that the private key may include any number of secret prime numbers $(P_1,P_2,P_3, \cdots P_n)$. Preferably, the secret prime numbers are selected according to the routine shown in FIGURE 3A. At step 35, an n-bit random number "x_1" is generated. The number of bits "n" needs to be large enough (eg, 250 bits) such that it is difficult to factor "M". At step 37, x_1 is incremented to be congruent to a predetermined value, eg, "3 mod 8". At step 39, a test is made to determine if x_1 is prime. If so, then the routine continues at step 41 by setting $x_1 = P_1$. If x_1 is not prime, then x_1 is incremented at step 43 (by setting $x_1 = x_1 + 8$) and the routine returns to step 39. Once P_1 is selected, the routine continues at step 45 to generate another n-bit random number "x_2". At step 47, x_2 is incremented to be congruent with a second predetermined value, eg, "7 mod 8". At step 49, a test is made to determine if x_2 is prime. If so, then the routine continues at step 51 by setting $x_2 = P_2$. If x_2 is not prime, then x_2 is incremented at step 53 (by setting $x_2 - x_2 + 8$) and the routine returns to step 49. Once P_2 is selected, the public key "M" is set equal to $P_1 \cdot P_2$ at step 55.

It is also desirable to store P_1 and P_2 in the issuing terminal responsible for computing signatures. Moreover, it is possible to distribute the private key (P_1,P_2) from one terminal to another without any person being able to discern the key by using another public-key cryptosystem pair (for which the private key is known only to the receiving terminal). Moreover, while the digital signing routine of FIGURE 3 is preferred, other schemes, such as RSA, the Goldwasser, Micall & Rivest scheme and/or the Rabin scheme, may be used. Such schemes may also require knowledge of the public key, although the routine of FIGURE 3 does not. In any case, the process of generating the "signature" is fast if the private key is known but is prohibitively slow otherwise. Any attempt to issue counter-

felt cards is complicated further by the use of a one-way function "F" to hash the password into the mapped password "Q". In this way, it becomes virtually impossible for a counterfeiter to mount a chosen-text attack on the card generation scheme even if the counterfeiter could somehow obstain signatures for fake personal data.

Referring now to FIGURE 4, a general flowchart diagram is shown of a preferred method for preventing unauthorized use of the personal identification card 10 issued according to the routines of FIGURES 2-3. At step 50, the personal identification card is received at a transaction terminal. At step 52, the encoded password/signature is decoded to generate a received password and a received signature. Preferably, the method Includes a step 54 wherein errors in the received password and received signature are corrected in accordance with well-known techniques. At step 56, the received password is mapped, with the same predetermined function "F" used at the issuing terminal, to generate a mapped password "Q_R" for the received personal identification card.

The routine then continues at step 58 to verify that the received signature is "valid". In particular, the method digitally verifies, using the public key of the public-key cryptosystem pair, whether the received signature can be generated from the mapped password "Q_R". If so, the method continues at step 60 to generate an indication that the received signature is valid. At step 62, a representation is generated from data in the received password. This representation will be a picture if the original password stored on the card included a digitized photograph of the authorized cardholder. Of course, step 62 can be performed in parallel with steps 58 and 60 so that the picture is immediately displayed while the signature verification takes place. Referring back to FIGURE 4, at step 64, the method displays either the pictorial representation or the indication, or both, on a display of the transaction terminal. This display is then verified by an operator of the terminal at step 66 to insure that the cardholder is authorized to effect a transaction.

It should be appreciated that the personal identification card generated according to the method of FIGURE 2 can be used in any situation requiring user identification. For example, and not by way of limitation, the authorized user can present the card to an authorized salesperson for charging a purchase. The salesperson would enter the card into the transaction terminal which is capable of reading the date from the card's memory, verifying that the (digital) signature on the card is valid, and displaying on the display screen information derived from the password. The salesperson can therefore be assured that the cardholder's identity is as claimed and proceed with the charge.

Referring now to FIGURE 5, a detailed flowchart is shown of the preferred digital verification routine of FIGURE 3. At step 68, the routine multiplies the mapped password "Q_R" from the received personal identification card by each of the factors ± 1 mod M and ± 2 mod M. The method continues at step 70 by squaring modulo "M" the received signature to generate a value "X". At step 72, a test is made to determine whether "X" equals either $\pm Q_R$ mod M or $\pm 2Q_R$ mod M. If so, the routine continues at step 74 to generate the indication that the received signature is valid. If "x" does not equal any one of these four factors, the signature is invalid and the transaction is inhibited.

Of course, the method and system of the present invention is easily adaptable to a multi-issuer scenario where several parties desire to issue cards using different cryptosystem pairs, but where verifiers (ie, operators of transaction terminals) need to authenticate a card from any of the issuers. This can be accomplished by encoding the public key used by each Issuer into each transaction terminal and then requiring the operator thereof to enter into the terminal both the identity of the issuer along with the card itself; alternatively, the identity of the card issuer can be encoded on the card. This type of system is shown in FIGURE 6, wherein a plurality of issuing terminals 76a...76n are provided for one or more independent issuers of authorized personal identification cards. Each of the independent issuers is assigned or selects a distinctive public-key cryptosystem pair unknown to the other issuers. As noted above, the public key of each such pair is then encoded into each of the one or more transaction terminals 78a...78n which are shared by all of the issuers.

The system of FIGURE 6 is useful for passport control, national identification cards, or multi-company credit cards, although such applications are not meant to be limiting. In operation of a passport system, for example, each country would have complete autonomy over the personal identification cards it issues, but a single transaction terminal would be used to authenticate the signature (which could include a visa) of any country.

Although not described in detail, it can be appreciated by those skilled in the art that the method and system of the present invention can be readily implemented with preexisting hardware and software. In the preferred embodiment, and as shown in FIGURE 6, each of the issuing terminals 76 includes a microcomputer 80 and associated memory devices 82 for storing operating programs and application programs for carrying out the method steps of FIGURE 2. Input/output devices, such as a keyboard 84 and display 86, are provided for interfacing the terminal to the card issuer. Of course, one or more of the method steps (eg, the digital signing step, the mapping step and the encoding step) can be implemented in either gate array logic chips or software. Likewise, each of the transaction terminals 78 preferably includes a microprocessor 88, associated memory 90, and appro-

priate input/output devices such as cardreader 92, keyboard 94 and display 96.

While the above discussion relates specifically to protection schemes for personal identification cards, it should be appreciated that the password/signature security routines of the present invention may also be used where the personal data is transmitted over a communications channel as opposed to being stored on an identification card per se. Returning back to FIGURE 6, this aspect of the invention is achieved by providing a communications channel 100, eg, a telephone link via modems, between an issuing terminal 76b and a transaction terminal 78a.

In operation, the method steps of FIGURE 2 would be the same as previously described except that step 40 is deleted and a step of transmitting the encoded password/signature over the communications channel 100 is substituted therefor. Likewise, step 50 of the verification routine in FIGURE 4 is deleted and is substituted with a step whereby the information provided over the communications channel 100 is received at the transaction terminal and then processed according to the remainder of the steps in FIGURE 4. In this way, the password/signature method is used for personal identification where the medium for supporting and transmitting the password and the signature is the communications channel itself rather than the identification card.

Although the invention has been described and illustrated in detail, the same is by way of example only and should not be taken by way of limitation.

Claims

1. A system for issuing authorized personal identification cards (10) and for preventing unauthorized use thereof, comprising:

issuing terminal means (76) for issuing a plurality of personal identification cards (10); each of said cards having stored therein a first data string (20) with a portion (20a) thereof derived from a physical characteristic of an authorized user of the card, each of said cards (10) also having stored therein a signature (22) derived from a second data string (Q) using a private key (P_1,P_2) of a public-key cryptosystem pair, the public-key cryptosystem pair also having a public key (M), the second data string (Q) being derived from the first data string (20) using a predetermined one-way function (F) and having a length substantially less than the length of the first data string (20); and

transaction terminal means (78) including at least one transaction terminal for receiving a personal identification card (10) offered to effect a transaction using the transaction terminal, the personal identification card (10) having the first data string (20) and a received signature (22) stored therein, wherein the transaction terminal (78) comprises means, using the public key (M) of the public-key cryptosystem pair, for verifying that the received signature (22) can be generated from the first data string (20), means responsive to the verifying means for generating a representation from the first data string, and means for displaying (96) the representation and an indication of whether the received signature (22) can be generated from the first data string (20) to enable an operator of the transaction terminal (78) to verify that the user of the offered personal identification card (10) is authorized to effect a transaction.

2. A system according to Claim 1, wherein the issuing terminal means (76) includes at least one issuing terminal for one or more independent issuers of authorized personal identification cards (10), each of the independent issuers having a distinctive public-key cryptosystem pair unknown to the other issuers.

3. A system for allowing authorized users of personal identification cards (10) to effect transactions via at least one transaction terminal (78), comprising a plurality of cards (10) each having stored therein a signature (22) which is the digital signature of a second data string (Q), the second data string (Q) being derived from a first data string (20) derived from a physical characteristic associated with a respective user, the second data string (Q) being derived from the first data string (20) using a predetermined one-way function (F) and having a length substantially less than the length of the first data string (20), the signature (22) stored in each of said cards (10) having been derived with the same private key (P_1,P_2) of a public-key cryptosystem pair also having a public key (M); and at least one transaction terminal (78) having means for controlling:

(1) the retrieval of the first data string (20) and the signature (22) stored in an inserted card;

(2) the digital verification of the signature (22) with the use of the public key (M) of the public-key cryptosystem pair;

(3) the generation of a pictorial representation from the first data string (20); and

(4) the effecting of a transaction only if the signature (22) is verified and the pictorial representation matches the user.

4. A terminal (76) for initializing personal identification cards (10) to be used with at least one transaction terminal (78), each card (10) having a memory (16) therein, comprising means for assigning a first data string (20) having a portion

(20a) thereof which is derived from a physical characteristic of a user whose card is to be initialized, means for mapping the first data string (20) with a predetermined one-way function (F) to generate a second data string (Q) having a length substantially less than the length of the first data string (20), means for deriving a digital signature (22) from the second data string (Q), the signature of each user being derived with use of a private key (P_1,P_2) of a public-key cryptosystem pair also having a public key (M), and means for controlling the storing in a user card (10) of the respective derived digital signature (22).

5. A personal identification card (10) for use in effecting transactions via at least one transaction terminal (78), comprising a body portion (12), a memory (16) within said body portion for storing a signature (22), said signature (22) being the digital signature of a second data string (Q) derived from a first data string (20) having at least a portion (20a) thereof being derived from a physical characteristic of a respective card user, the second data string (Q) being derived from the first data string (20) using a predetermined one-way function (F) and having a length substantially less than the length of the first data string (20), wherein said signature (22) is derived from the second data string (Q) with the private key (P_1,P_2) of a public-key cryptosystem pair.

6. A method for enabling an authorized user of a personal identification card (10) to effect a transaction using a transaction terminal (78), the personal identification card (10) having user-characteristic data (20) derived from a physical characteristic of the authorized user and which need not be retained secret, and a signature (22) of the user-characteristic data (20) derived from a private key (P_1,P_2) of a public-key cryptosystem pair, the public-key cryptosystem pair also including a public key (M), comprising the steps of:

receiving the personal identification card (10) at the transaction terminal (78);

digitally verifying, using the public key (M), whether the signature (22) on the personal identification card (10) received at the transaction terminal (78) can be generated from the user-characteristic data (20); and

if the signature (22) can be generated from the user-characteristic data (20) using the public key (M), displaying a representation of the user-characteristic data (20) on a display (96) of the transaction terminal (78) to enable an operator thereof to verify that the user is authorised to effect a transaction using the personal card.

7. A method according to Claim 6, wherein both a representation of said physical characteristic of the authorized user, and an indication of the validity status of the signature (22) on the personal identification card (10) are displayed on a display of said transaction terminal (78), said representation being generated from the user-characteristic data (20) on the personal identification card (10).

8. A method according to Claim 6 or 7, wherein said signature (22) of the user-characteristic data (20) is derived by:

(i) generating an intermediate data string (Q) from the user-characteristic data using a predetermined one-way function (F), the intermediate data string (Q) being substantially smaller in size than said user-characteristic data; and

(ii) deriving said signature (22) from said intermediate data string (Q) using said private key (P_1,P_2).

Patentansprüche

1. System zur Ausgabe von autorisierten persönlichen Identifikationskarten (10) und zur Verhinderung ihrer unberechtigten Verwendung, welches enthält:
ein Ausgabeterminal (76) zur Ausgabe einer Vielzahl von persönlichen Identifikationskarten (10), wobei auf jeder der Karten eine erste Datenreihe (20) mit einem Teil (20a) gespeichert ist, der von physikalischen Charakteristika eines autorisierten Anwenders der Karte stammt, wobei jede der Karten (10) ferner eine Signatur (22) gespeichert aufweist, die von einer zweiten Datenreihe (Q) unter Verwendung eines privaten Schlüssels (P_1, P_2) eines offenen Krpytosystempaars enthält, wobei das offene Kryptosytempaar außerdem einen offenen Schlüsel (M) aufweist, wobei die zweite Datenreihe (Q) aus der ersten Datenreihe (20) abgeleitet ist, in dem eine vorbestimmte Einwegfunktion (F) verwendet ist und die eine Länge aufweist, die beträchtlich kleiner als die Länge der ersten Datenreihe (20) ist; und mit einem Übertragungsterminal (78), das wenigstens ein Übertragungsterminal zur Aufnahme einer persönlichen Identifikationskarte (10) enthält, mit der eine Übertragung unter Verwendung des Übertragungsterminals möglich ist, wobei die persönliche Identifikationskarte (10) eine erste Datenreihe (20) und eine darin aufgenommene Signatur (22) enthält, wobei das Übertragungsterminal (78) Mittel enthält, welche den offenen Schlüssel (M) des Offen-Schlüssel-Kryptosystempaars verwenden, um sicherzustellen, daß die empfangene Signatur (22) aus der ersten Da-

tenreihe (20) abgeleitet werden kann, Mittel, die auf die Überprüfungsmittel ansprechen, um eine Darstellung aus der ersten Datenreihe zu erzeugen, und Mitteln zur Anzeige (96) der Darstellung und eine Anzeige, ob die empfangene Signatur (22) aus der ersten Datenreihe (20) erzeugt werden kann, um einem Bediener des Übertragungsterminals (78) zu bestätigen, daß der Verwender der angebotenen persönlichen Identifikationskarte (10) autorisiert ist, die Übertragung zu bewirken.

2. System nach Anspruch 1, bei dem das Ausgabeterminal (76) wenigstens ein Ausgabeterminal für einen oder mehrere unabhängige Ausgeber von autorisierten persönlichen Identifikationskarten (10) enthält, wobei jede der unabhängigen Ausgeber ein bestimmtes Offen-Schlüssel-Kryptosystempaar verwendet, das den anderen Ausgebern unbekannt ist.

3. System, es autorisierten Verwendern von persönlichen Identifkationskarten (10) zu ermöglichen, eine Übertragung über wenigstens ein Übertragungsterminal (78) zu bewirken, das eine Vielzahl von Karten (10) enthält, die jeweils eine Signatur (22) aufweisen, welche die digitale Signatur einer zweiten Datenreihe (Q) ist, wobei die zweite Datenreihe (Q) aus einer ersten Datenreihe (20) abgeleitet ist, die von physikalischen Charakteristika bezüglich des entsprechenden Nutzers abgeleitet ist und wobei die zweite Datenreihe (Q) aus der ersten Datenreihe (20) unter Verwendung einer vorbestimmten Einwegfunktion (F) abgeleitet ist und eine Länge aufweist, die beträchtlich geringer als die Länge der ersten Datenreihe (20) ist, wobei die Signatur (22), die in jeder der Karten (10) gespeichert ist, mit dem gleichen privaten Schlüssel (P_1, P_2) eines Offen-Schlüssel-Kryptosystempaars abgeleitet ist, das ebenfalls einen offenen Schlüssel (M) aufweist, und mit wenigstens einem Übertragungsterminal (78), mit Mitteln zur Steuerung

(1) des Ermittelns der ersten Datenreihe (20) und der Signatur (22), die auf der Karte gespeichert sind,

(2) der digitalen Verifikation der Signatur (22) unter Verwendung des offenen Schlüssels (M) des Offen-Schlüssel-Kryptosystempaars,

(3) der Erzeugung einer Bilddarstellung aus der ersten Datenreihe (20) und

(4) der Bewirkung einer Übertragung, nur dann, wenn die Signatur (22) verifiziert ist und die bildliche Darstellung dem Anwender entspricht.

4. Terminal (76) zur Initialisierung persönlicher Identifikationskarten (10) zur Verwendung mit wenigstens einem Übertragungsterminal (78), wobei jede Karte (10) einen Speicher (16) enthält, mit Mitteln zur Zuordnung einer ersten Datenreihe (20) mit einem Teil (20a), der aus physikalischen Charakteristika eines Verwenders abgeleitet ist, dessen Karte zur initialisieren ist, Mitteln zur Abbildung der ersten Datenreihe (20) mit einer vorbestimmten Einwegfunktion (F) zur Erzeugung einer zweiten Datenreihe (Q) mit einer Länge, die beträchtlich kleiner als die Länge der ersten Datenreihe (20) ist, Mitteln zur Ableitung einer digitalen Signatur (22) aus der zweiten Datenreihe (Q), wobei die Signatur jedes Verwenders unter Verwendung eines privaten Schlüssels (P_1, P_2) eines Offen-Schlüssel-Kryptosystempaars abgeleitet ist, das außerdem einen offenen Schlüssel (M) aufweist, und Mitteln zur Steuerung der Speicherung auf der Anwenderkarte (10) der entsprechend abgeleiteten digitalen Signatur (22).

5. Eine persönliche Identifikationskarte (10) zur Verwendung bei der Auslösung von Übertragungen über wenigstens ein Übertragungsterminal (78), die einen Grundkörper (12) enthält, einen Speicher (16) innerhalb des Grundkörperteils zur Speicherung einer Signatur (22), wobei die Signatur (22) die digitale Signatur einer zweiten Datenreihe (Q) ist, die aus einer ersten Datenreihe (20) abgeleitet ist, die wenigstens ein Teil (20a) dieser enthält, der aus einer physikalischen Charakteristik des entsprechenden Kartenverwenders abgeleitet ist, wobei die zweite Datenreihe (Q) aus der ersten Datenreihe (20) unter Verwendung einer vorbestimmten Einwegfunktion (F) abgeleitet ist und eine Länge aufweist, die beträchtlich kleiner als die Länge der ersten Datenreihe (20) ist, wobei die Signatur (22) aus der zweiten Datenreihe (Q) mit dem privaten Schlüssel (P_1, P_2) eines Offen-Schlüssel-Kryptosystems abgeleitet ist.

6. Verfahren zur Bewirkung einer Übertragung durch einen autorisierten Verwender einer persönlichen Identifikationskarte (10) unter Verwendung eines Übertragungsterminals (78), wobei die persönliche Identifikationskarte (10) anwendercharakteristische Daten (20) enthält, die aus physikalischen Charakteristika des autorisierten Verwenders abgeleitet sind und die nicht geheim zu halten sind, und einer Signatur (22) der anwendercharakteristischen Daten (20), die von einem privaten Schlüssel (P_1, P_2) eines Offen-Schlüssel-Kryptosystempaars abgeleitet ist, wobei das Offen-Schlüssel-Kryptosystempaar außerdem einen offenen Schlüssel (M) enthält, das die Schritte umfaßt: Annahme der persönli-

chen Identifkationskarte (10) an dem Übertragungsterminal (78), digitale Verifizierung unter Verwendung des offenen Schlüssels (M), ob die Signatur (22) auf der persönlichen Identifikationskarte (10), die vom Übertragungsterminal (78) aufgenommen ist, aus den anwendercharakteristischen Daten (20) erzeugt werden kann, und wenn die Signatur (22) aus den anwendercharakteristischen Daten (20) unter Verwendung des offenen Schlüssels (M) abgeleitet werden kann, Anzeige einer Darstellung der anwendercharakteristischen Daten (20) auf einem Display (96) des Übertragungsterminals (78), um dessen Bediener zu ermöglichen zu verifizieren, daß der Verwender berechtigt ist, eine Übertragung unter Verwendung der persönlichen Karte vorzunehmen.

7. Verfahren nach Anspruch 6, bei dem sowohl eine Darstellung der physikalischen Charakteristika des autorisierten Verwenders, und eine Anzeige des Gültigkeitsstatus der Signatur (22) auf der persönliche Identifkationskarte (10) auf einem Display des Übertragungsterminals (78) angezeigt werden, wobei die Darstellung aus den anwendercharakteristischen Daten (20) auf der persönlichen Identifikationskarte (10) erzeugt ist.

8. Verfahren nach Anspruch 6 oder 7, bei dem die Signatur (22) der anwendercharakteristischen Daten (20) abgeleitet sind durch
   (i) Erzeugen einer Zwischendatenreihe (Q) aus den anwendercharakteristischen Daten unter Verwendung einer vorbestimmten Einwegfunktion (F), wobei die Zwischendatenreihe (Q) beträchtlich kleiner in der Größe ist als die anwendercharakteristischen Daten ist, und
   (ii) Ableiten der Signatur (22) aus der Zwischendatenreihe (Q) unter Verwendung eines privaten Schlüssels (P_1, P_2).

Revendications

1. Système servant à produire des cartes d'identification pour personnel autorisé (**10**) et à empêcher leur utilisation par du personnel non autorisé, comprenant :
   un moyen de production à terminal (**76**) servant à produire une pluralité de cartes d'identification de personnel (**10**) ; chacune desdites cartes ayant stocké, en son sein, une première suite de données (**20**), avec une partie (**20a**) de cette dernière déduite d'une caractéristique physique d'un utilisateur autorisé de la carte, chacune desdites cartes (**10**) ayant également, stocké en son sein, une empreinte numérique (**22**) déduite d'une deuxième suite de données (**Q**) utilisant une clé privée (P_1, P_2) d'un couple de système de chiffrage à clé publique, le système de chiffrage à clé publique ayant également une clé publique (**M**), la deuxième suite de données (**Q**) étant déduite de la première suite de données (**20**) à l'aide d'une fonction univoque prédéterminée (**F**) et ayant une longueur sensiblement inférieure à la longueur de la première suite de données (**20**) ; et
   un moyen de mouvement à terminal (**78**), comprenant au moins un terminal de mouvement destiné à recevoir une carte d'identification de personnel (**10**) présentée afin d'effectuer un mouvement à l'aide d'un terminal de mouvement, la carte d'identification de personnel (**10**) présentant la première suite de données (**20**) et une empreinte (**22**) reçue, stockée en son sein, dans lequel le terminal de mouvement (**78**) comprend un moyen, utilisant la clé publique (**M**) du couple de système de chiffrage à clé publique, servant à vérifier que l'empreinte (**22**) reçue peut être produite par la première suite de données (**20**), un moyen réagissant au moyen de vérification, afin de produire une représentation à partir de la première suite de données, et un moyen (**96**) servant à afficher la représentation et une indication du fait que l'empreinte (**22**) reçue peut être produite par la première suite de données (**20**), afin de permettre à un opérateur du terminal de mouvement (**78**) de vérifier que l'utilisateur de la carte d'identification de personnel (**10**) présentée est autorisé à effectuer un mouvement.

2. Système selon la revendication 1, dans lequel le moyen de production à terminal (**76**) comprend au moins un terminal de production pour un ou plusieurs émetteurs indépendants de cartes d'identification de personnel autorisé (**10**), chacun des émetteurs indépendants présentant un couple de système de chiffrage à clé publique distinctive, inconnu des autres émetteurs.

3. Système servant à permettre à des utilisateurs autorisés de cartes d'identification de personnel (**10**) d'effectuer des mouvements via au moins un terminal de mouvement (**78**), comprenant une pluralité de cartes (**10**), présentant chacune, en son sein, une empreinte (**22**), qui est l'empreinte numérique d'une deuxième suite de données (**Q**), la deuxième suite de données (**Q**) étant déduite d'une première suite de données (**20**), déduite d'une caractéristique physique associée à un utilisateur respectif, la deuxième suite de données (**Q**) étant déduite de la première suite de données (**20**) à l'aide d'une fonction univoque prédéterminée (**F**) et ayant une longueur sensiblement inférieure à la longueur de la première suite de don-

nées (**20**), l'empreinte (**22**), stockée dans chacune desdites cartes (**10**), ayant été déduite avec la même clé privée (P_1, P_2) d'un couple de système de chiffrage à clé publique ayant une clé publique (**M**) ; et au moins un terminal de mouvement (**78**) présentant un moyen servant à commander :

(**1**) l'extraction de la première suite de données (**20**) et de l'empreinte (**22**) stockée dans une carte insérée;

(**2**) la vérification numérique de l'empreinte (**22**) à l'aide de la clé publique (**M**) du couple de système de chiffrage à clé publique ;

(**3**) la production d'une représentation graphique de la première suite de données (**20**) ; et

(**4**) la réalisation d'un mouvement, seulement si l'empreinte (**22**) est vérifiée et que la représentation graphique est adaptée à l'utilisateur.

4. Terminal (**76**) d'initialisation de cartes d'identification de personnel (**10**), destiné à être utilisé avec au moins un terminal de mouvement (**78**), chaque carte (**10**) ayant, en son sein, une mémoire (**16**), comprenant un moyen servant à attribuer une première suite de données (**20**), dont une partie (**20a**) est déduite d'une caractéristique physique d'un utilisateur dont la carte doit être initialisée, un moyen servant à tracer une carte de la première suite de données (**20**) avec une fonction univoque prédéterminée (**F**), afin de produire une deuxième suite de données (**Q**) ayant une longueur sensiblement inférieure à la longueur de la première suite de données (**20**), un moyen servant à déduire une empreinte numérique (**22**) à partir de la deuxième suite de données (**Q**), l'empreinte de chaque utilisateur étant déduite d'une clé privée (P_1, P_2) d'un couple de système de chiffrage à clé publique ayant également une clé publique (**M**), et un moyen servant à commander le stockage d'une carte d'utilisateur (**10**) de l'empreinte numérique (**22**) déduite respective.

5. Carte d'identification de personnel (**10**) destinée à être utilisée afin d'effectuer des mouvements via au moins un terminal de mouvement (**78**), comprenant une partie de corps (**12**), une mémoire (**16**) dans ladite partie de corps afin de stocker une empreinte (**22**), ladite empreinte (**22**) étant l'empreinte numérique d'une deuxième suite de données (**Q**) déduite d'une première suite de données (**20**), ayant au moins une partie (**20a**) déduite d'une caractéristique physique d'un utilisateur de carte respectif, la deuxième suite de données (**Q**) étant déduite de la première suite de données (**20**) à l'aide d'une fonction univoque prédéterminée (**F**) et ayant une longueur sensiblement inférieure à la longueur de la première suite de données (**20**), dans laquelle ladite empreinte (**22**) est déduite de la deuxième suite de données (**Q**) avec la clé privée (P_1, P_2) d'un couple de système de chiffrage à clé publique.

6. Procédé servant à permettre à un utilisateur autorisé d'une carte d'identification de personnel (**10**) d'effectuer un mouvement à l'aide d'un terminal de mouvement (**78**), la carte d'identification de personnel (**10**) ayant des données de caractéristique d'utilisateur (**20**) déduites d'une caractéristique physique de l'utilisateur autorisé et ne nécessitant pas d'être maintenues secrètes, et une empreinte (**22**) des données de caractéristique d'utilisateur (**20**) déduites d'une clé privée (P_1, P_2) d'un couple de système de chiffrage à clé publique, le couple de système de chiffrage à clé publique comportant également une clé publique (**M**), procédé comprenant les étapes de :

réception de la carte d'identification de personnel (**10**) au terminal de mouvement (**78**) ;

vérification numérique, à l'aide de la clé publique (**M**), du fait que l'empreinte (**22**) située sur la carte d'identification de personnel (**10**), reçue au terminal de mouvement (**78**), peut être produite à partir des données de caractéristique d'utilisateur (**20**) ; et

si l'empreinte (**22**) peut être produite à partir des données de caractéristique d'utilisateur (**20**) à l'aide de la clé publique (**M**), affichage d'une représentation des données de caractéristique d'utilisateur (**20**) sur un affichage (**96**) du terminal de mouvement (**78**), afin de permettre à son opérateur de vérifier que l'utilisateur est autorisé à effectuer un mouvement à l'aide de la carte de personnel.

7. Procédé selon la revendication 6, dans lequel, à la fois, une représentation de ladite caractéristique physique de l'utilisateur autorisé et une indication de l'état de validité de l'empreinte (**22**) sur la carte d'identification de personnel (**10**) sont affichées sur un affichage dudit terminal de mouvement (**78**), ladite représentation étant produite à partir des données de caractéristique d'utilisateur (**20**) situées sur la carte d'identification de personnel (**10**).

8. Procédé selon la revendication 6 ou 7, dans lequel ladite empreinte (**22**) des données de caractéristique d'utilisateur (**20**) est déduite :

(i) en produisant une suite de données (**Q**) intermédiaire à partir des données de caractéristique d'utilisateur, à l'aide d'une fonction univoque prédéterminée (**F**), la taille de la suite de données (**Q**) intermédiaire étant sensiblement inférieure à celle desdites données de caractéristique d'utilisateur ; et

(ii) en déduisant ladite empreinte (**22**) à partir de ladite suite de données (**Q**) intermédiaire à l'aide de ladite clé privée (P_1, P_2).

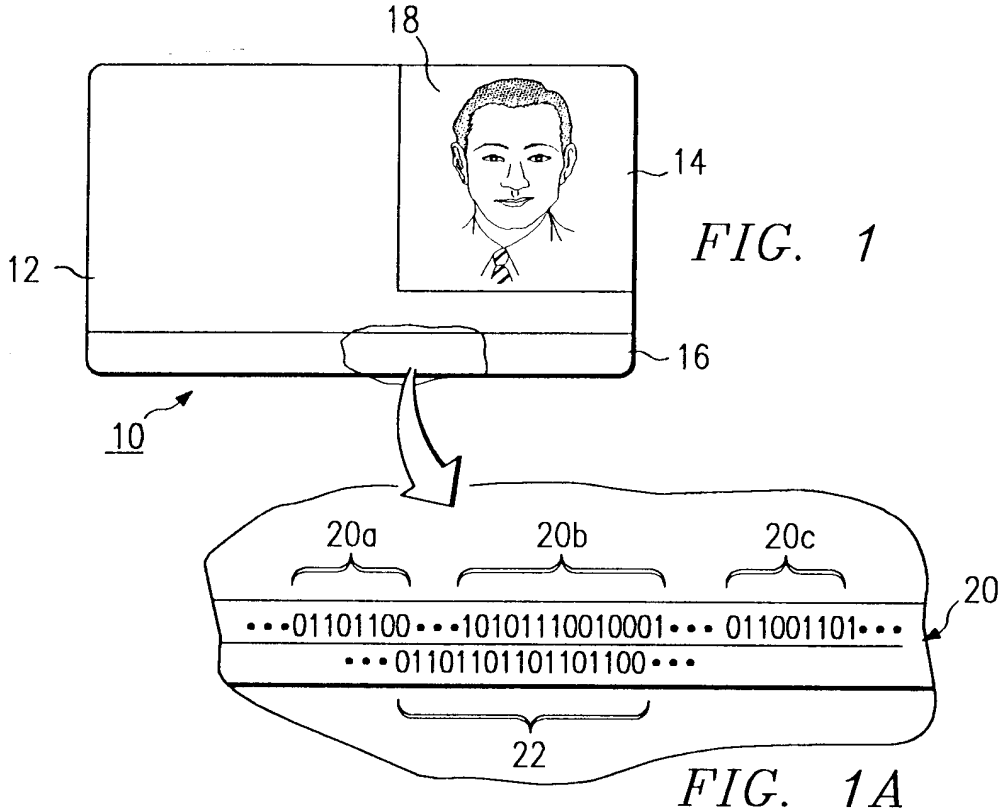

FIG. 1

FIG. 1A

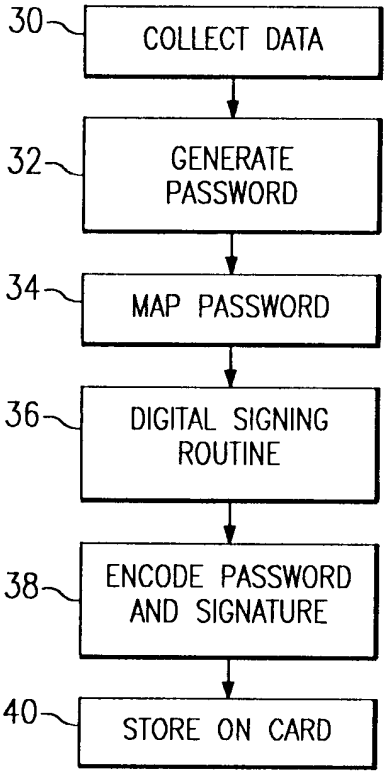

FIG. 2

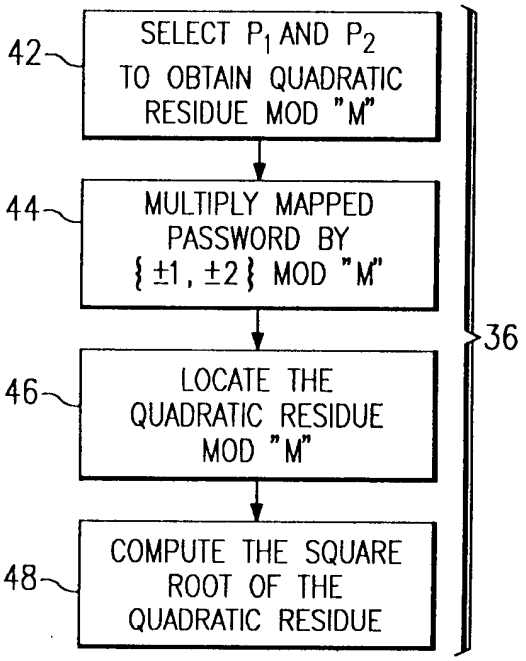

FIG. 3

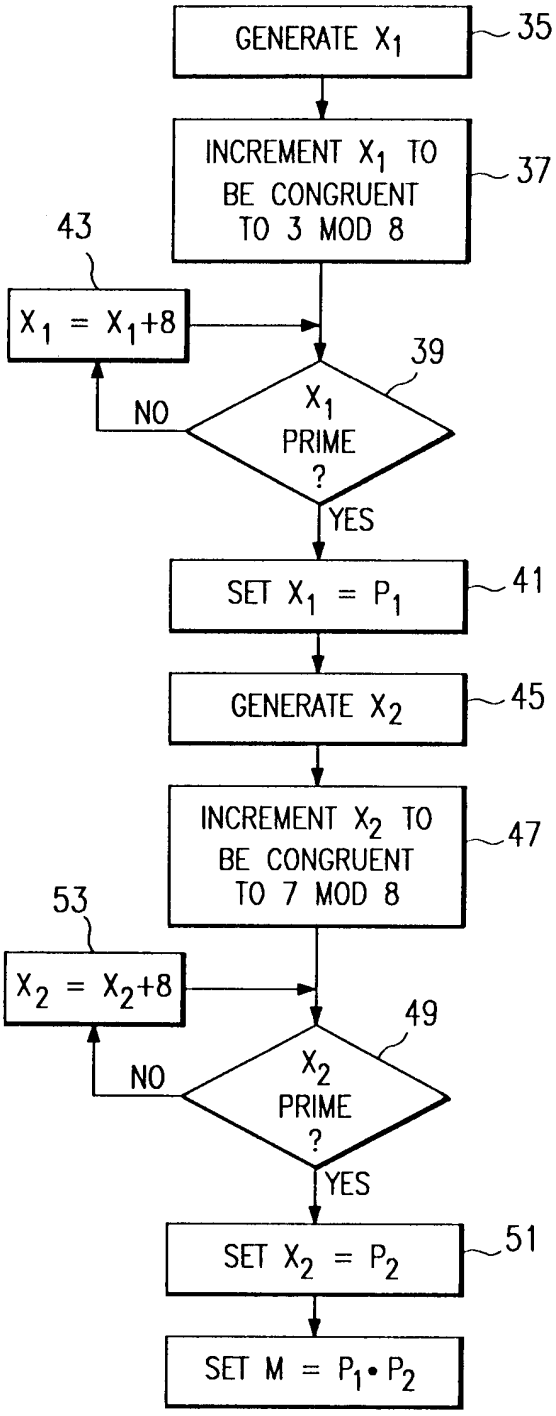
GENERATE X_1
35
INCREMENT X_1 TO BE CONGRUENT TO 3 MOD 8
37
43
$X_1 = X_1+8$
39
X_1 PRIME ?
NO
YES
SET $X_1 = P_1$
41
GENERATE X_2
45
INCREMENT X_2 TO BE CONGRUENT TO 7 MOD 8
47
53
$X_2 = X_2+8$
49
X_2 PRIME ?
NO
YES
SET $X_2 = P_2$
51
SET $M = P_1 \cdot P_2$

FIG. 3A

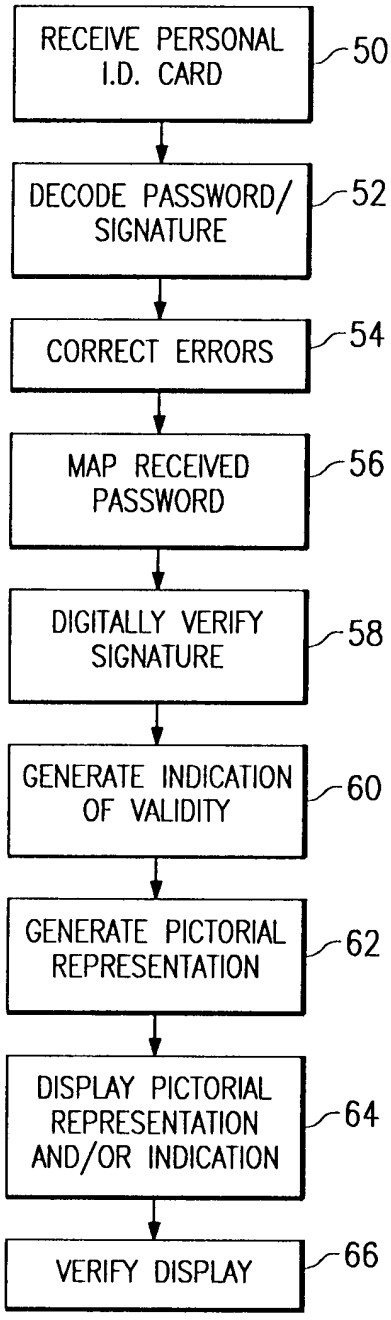
RECEIVE PERSONAL I.D. CARD
50
DECODE PASSWORD/ SIGNATURE
52
CORRECT ERRORS
54
MAP RECEIVED PASSWORD
56
DIGITALLY VERIFY SIGNATURE
58
GENERATE INDICATION OF VALIDITY
60
GENERATE PICTORIAL REPRESENTATION
62
DISPLAY PICTORIAL REPRESENTATION AND/OR INDICATION
64
VERIFY DISPLAY
66

FIG. 4

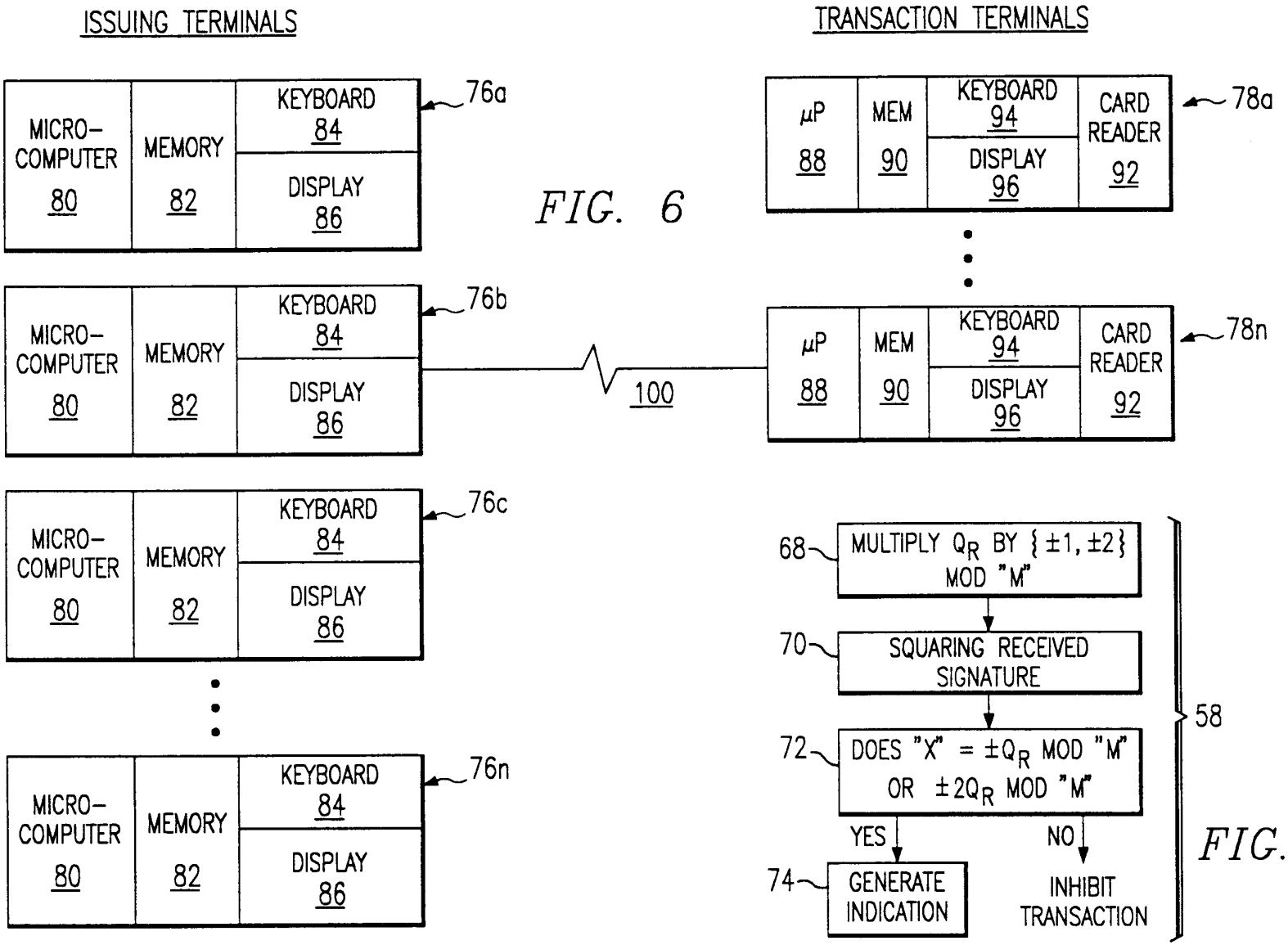
ISSUING TERMINALS
TRANSACTION TERMINALS
MICRO-COMPUTER 80
MEMORY 82
KEYBOARD 84
DISPLAY 86
76a
76b
76c
76n
μP 88
MEM 90
KEYBOARD 94
DISPLAY 96
CARD READER 92
78a
78n
100

FIG. 6

68
MULTIPLY Q_R BY {±1, ±2} MOD "M"
70
SQUARING RECEIVED SIGNATURE
72
DOES "X" = $\pm Q_R$ MOD "M" OR $\pm 2Q_R$ MOD "M"
YES
NO
74
GENERATE INDICATION
INHIBIT TRANSACTION
58

FIG. 5